

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-046305

(43)Date of publication of application : 12.02.2004

(54)Int.Cl.

G07C 1/20

(21)Application number : 2002-199415

(71)Applicant : AMANO CORP

(22)Date of filing : 09.07.2002

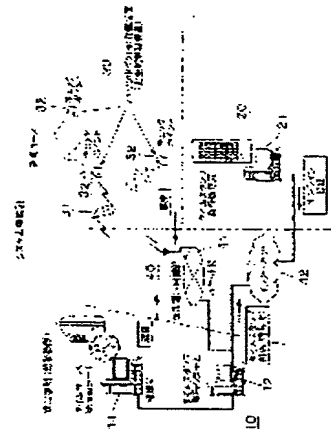
(72)Inventor : YOKOYAMA SUMIAKI

(54) PATROL RECORDER SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a simple but reliable patrol recorder system that can certify and authenticate a patrol duty.

SOLUTION: A portable patrol radio 31 requests a checkpoint ID transmitter 32 to transmit a checkpoint ID, and the checkpoint ID transmitter 32 validates the requester to deliver a checkpoint ID to the patrol. The portable patrol radio 31 transmits the checkpoint ID and a portable radio ID to a time stamp issuing server 12 to request a time stamp. The time stamp issuing server 12 validates the request to generate a time stamp from the standard time, and transmits it to a time stamp issue requester 21 in a patrol data management center 10. The time stamp issue requester 21 saves the transmitted time stamp object, and copies patrol data from the time stamp object to use them as a patrol record.



LEGAL STATUS

[Date of request for examination]

27.05.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

BEST AVAILABLE COPY

THIS PAGE BLANK (USPTO)

* NOTICES *

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1]

It is the patrol recorder system consisted of the time stamp processing center which carries out issue processing of the time stamp, a round data-control pin center, large which manages the data which the round member patrolled and obtained while carrying out the issue request of the time stamp in the above-mentioned time stamp processing center, and a round field which a round member should patrol, and a round member possessed a portable remote terminal machine, and transmitted the positional information and its round time of day of the checkpoint which patrolled and patrolled in a checkpoint to a record machine, and constituted so that it may record, It consists of a field radio for a round, a checkpoint ID sender formed in the round location, and a time stamp issue server, an ID call means to by which the above-mentioned field radio for a round calls an ID code to the above-mentioned checkpoint ID sender by wireless, an ID code receiving means receive the checkpoint ID code to which it is sent from a checkpoint ID sender in response to this ID call, and the checkpoint ID and the field radio ID for a round, with which it has been sent -- and -- or a time stamp issue demand means give the demand which should send a round member ID on radio to the above-mentioned time stamp issue server, and should carry out a time stamp to a time stamp issue server -- having

The above-mentioned checkpoint ID sender has the ID code storage means which shows a round location, and a round location ID dispatch means to answer ID call from the above-mentioned field radio for a round, and to send ID,

It has a time stamp object issue means for the above-mentioned time stamp issue server to add the time of day to the clock means which minces standard time of day, and the above-mentioned ID code sent from the field radio for a round, and to generate the enciphered time stamp object, and to transmit to a predetermined server,

The patrol recorder system characterized by things.

[Claim 2]

the configuration of a time stamp object -- time stamp information, the round location ID, and the field radio ID for a round -- and -- or the patrol recorder system according to claim 1 characterized by to consist of text information containing the round member ID or related information, encryption information for online verification enciphered with the private key for independent organization verification in the above-mentioned text information, and information which were enciphered with the private key for off-line verification in the above-mentioned text information.

[Claim 3]

It is the patrol recorder system according to claim 1 or 2 characterized by for the above-mentioned time stamp processing center consisting of an issue processing time stamp [time stamp] issue server based on the time of day which the time server which supplies standard time of day, and this time server supply, and the above-mentioned round data control pin center, large consisting of time stamp issue request origin which requests a time stamp from the time stamp issue server of the above-mentioned time stamp processing center.

[Claim 4]

The cooperation time server with which the above-mentioned round data control pin center, large cooperates to the time server of the above-mentioned time stamp processing center further, It consists of a cooperation time stamp issue server which cooperates with the above-mentioned time stamp issue server. The above-mentioned field radio for a round An ID call means to call an ID code to the above-mentioned checkpoint ID sender by wireless, An ID code receiving means to receive the checkpoint ID code sent from a checkpoint ID sender in response to this ID call, Or the round member ID is sent on radio to the time stamp issue server which cooperates with the time stamp issue server of the above-mentioned time stamp processing center. the checkpoint ID and the field radio ID for a round which have been sent -- and -- And the patrol recorder system according to claim 1, 2, or 3 characterized by having a time stamp issue demand means to perform the demand which should carry out a time stamp.

[Translation done.]

THIS PAGE BLANK (US770)

* NOTICES *

JPO and NCIP are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.*** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

{Detailed Description of the Invention}

[0001]

{Field of the Invention}

This invention relates to the patrol recorder system which is used for the crime prevention defense patrol of works, a warehouse or a building, and various facilities called a school etc., and records the time of day in each round part, and enables the certification.

[0002]

{Description of the Prior Art}

There is a "round recording device" looked at as a conventional patrol recorder system by JP,61-82288,A proposed by these people. This equipment is a pocket-type patrol recorder system, records round time of day in a recorder, and became the above-mentioned patrol recorder system in the central unit with the code of a record round part, and the configuration of collecting round time-of-day data while a position code was attached from the code machine installed during the round in the round location.

[0003]

Moreover, the "building management equipment" of a publication exists in JP,9-305813,A. This equipment is the system have a round time-amount calculation means receives the above-mentioned location change information to the above-mentioned management equipment, and compute the round time amount of the above-mentioned customer engineer, detect positional information from a pocket machine, and collect a round location and round time amount in the equipment with which the management equipment connected with the private-branch-exchange equipment which transmits the location change information which shows change of the location of the pocket machine which a customer engineer possesses, and this private branch exchange by the telephone line was installed.

[0004]

{Problem(s) to be Solved by the Invention}

In the above-mentioned conventional system, to the alteration of time of day based on the accuracy of time of day, and malice, dependability cannot be set at all, and there is a problem which cannot give the guarantee to round implementation.

That is, even if record of a time stamp was the time of day synchronized by the clock which patrol recorder equipment contains or the GPS clock, and the electric-wave clock, it was not what does not prove having synchronized with it and a third person accepts.

Moreover, in text data, when the company and organization which contracted defense etc. proved having gone round truly, even if it was the time stamp which the time of day managed in the company and organization which contracted, and an independent organization (certificate authority) published, since it may have altered, it was not what can prove bona fides. Furthermore, it was not what may be able to alter other round data similarly and can prove bona fides.

[0005]

Furthermore, although the method which uses a cellular phone or a digital cordless phone, adds location information by GPS, and requires a time stamp of an independent organization is also considered, since the location information by GPS is public information, spoofing (alteration) of a location is possible for it, and it cannot prove bona fides.

Moreover, although there is also a method with which a cellular phone or a digital cordless phone is used, and an independent organization catches the location by GPS, the location prehension by GPS has problems, like the alternative system which catches a location is needed, in order for there to be also many environments which cannot be caught [inside / of an underground center and a building] and to pinpoint a location.

[0006]

This invention is a thing which devised so that it might be made in view of the above-mentioned trouble, the purpose might give the guarantee to round implementation and bona fides could be proved and for which it simplifies and a reliable patrol recorder system is offered.

[0007]

{Means for Solving the Problem}

In order to attain the above-mentioned purpose, the patrol recorder system of this invention While carrying out the issue request of said time stamp processing center according to claim 1 which carries out issue processing of like and the time stamp, and the time stamp in the above-mentioned time stamp processing center The round data control pin center,large which manages the data which the round member patrolled and obtained, Consist of a round field which a round member should patrol, and a round member possesses a portable remote terminal machine, and patrols a checkpoint. It is the patrol recorder system constituted so that the positional information and its round time of day of the patrolled checkpoint might be transmitted and recorded on a record machine. The field radio for a round, It consists of a checkpoint ID sender formed in the round location, and a time stamp issue server. The above-mentioned field radio for a round An ID call means to call an ID code to the above-mentioned checkpoint ID sender by wireless, An ID code receiving means to receive the checkpoint ID code sent from a checkpoint ID sender in response to this ID call, Or the round member ID is sent on radio to the above-mentioned time stamp issue server. the checkpoint ID and the field radio ID for a round which have been sent -- and -- It has a time stamp issue demand means to give the demand which should carry out a time stamp to a time stamp issue server. And the above-mentioned checkpoint ID sender It has the ID code storage means which shows a round location, and a round location ID dispatch means to answer ID call from the above-mentioned field radio for a round, and to send ID. The above-mentioned time stamp issue server The time of day is added to the clock means which minces standard time of day, and the above-mentioned ID code sent from the field radio for a round, and

THIS PAGE BLANK (USPTO)

it is characterized by having a time stamp object issue means to generate the enciphered time stamp object and to transmit to a predetermined server.

[0008]

moreover, the patrol recorder system of this invention -- said -- being according to claim 2 -- the configuration of like and a time stamp object -- time stamp information, a round location ID, and the field radio ID for a round -- and -- or it is characterized by to consist of text information containing the round member ID or related information, encryption information for online verification enciphered with the private key for independent organization verification in the above-mentioned text information, and information enciphered with the private key for off-line verification in the above-mentioned text information.

[0009]

Furthermore, the patrol recorder system of this invention is characterized by said like and the above-mentioned time stamp processing center consists of an issue processing time stamp [time stamp] issue server based on the time of day which the time server which supplies standard time of day, and this time server supply, and the above-mentioned round data control pin center,large consists of time stamp issue request origin which requests a time stamp from the time stamp issue server of the above-mentioned time stamp processing center according to claim 3.

[0010]

Furthermore, the patrol recorder system of this invention To said claim 4, like a publication the above-mentioned round data control pin center,large Furthermore, the cooperation time server which cooperates to the time server of the above-mentioned time stamp processing center, It consists of a cooperation time stamp issue server which cooperates with the above-mentioned time stamp issue server. The above-mentioned field radio for a round An ID call means to call an ID code to the above-mentioned checkpoint ID sender by wireless, An ID code receiving means to receive the checkpoint ID code sent from a checkpoint ID sender in response to this ID call, Or the round member ID is sent on radio to the time stamp issue server which cooperates with the time stamp issue server of the above-mentioned time stamp processing center. the checkpoint ID and the field radio ID for a round which have been sent -- and -- And it is characterized by having a time stamp issue demand means to perform the demand which should carry out a time stamp.

[0011]

According to this invention which consists of each above-mentioned means, the checkpoint ID sender using the short-distance wireless technique which sends the checkpoint ID (positional information) of a proper is installed in each round checkpoint, respectively, and a round member goes round with field radios, such as a digital cordless phone with a cellular phone with short-distance wireless, or a short-distance sender. A round member advances the Request to Send of a checkpoint ID (positional information) from a field radio to a checkpoint ID sender by the checkpoint, and a checkpoint ID sender checks the effectiveness of a claimant, and when effective, it distributes a checkpoint ID to a round member.

[0012]

next -- if a field radio receives a checkpoint ID -- automatic -- a time stamp issue server -- a checkpoint ID and a field radio ID -- and -- or the round member ID is transmitted and a time stamp is required of a time stamp issue system. It generates a time stamp from standard time of day, and transmits it to round data control pin center,large time stamp issue request-origin while the time stamp issue server of which the time stamp was required checks the effectiveness of a demand, and it answers a letter in confirmation-of-receipt information, when effective. Time stamp issue request origin saves the sent time stamp (object), posts round data from a time stamp object, and utilizes them as round record.

[0013]

moreover, the information which transmitted the time stamp object to the time stamp processing center which is an independent organization (certificate authority) by the communication link, and was enciphered for verification in verification of the bona fides of round data -- a decryption (private key) -- collating and verification of are done and a letter is answered in a verification result on-line. Moreover, when verification by the time stamp issue request origin itself is needed on employment and business, by adding the information which enciphered round data with the key for off-line verification to a time stamp object, it is time stamp issue request origin, and makes it possible to use and collate and verify the decode key for off-line verification currently exhibited.

[0014]

[Embodiment of the Invention]

Below, the patrol recorder system by the example of this invention is explained, referring to a drawing. Drawing 1 shows the outline configuration of the patrol recorder system by the example of this invention, and ten are a round field where, as for the time stamp processing center as an external engine, and 20, a round member patrols the round data control pin center,large of a client side, and 30 patrols each checkpoint among drawing. The time stamp processing center 10 consists of the time server 11 and the time stamp issue server 12 which synchronize with universal time, and verifies a time stamp. The time server 11 by the side of a pin center,large synchronizes with universal time coordinated, and distributes time of day to the time stamp issue server 12. To the time stamp issue demand demanded from the field radio 31 for a round which is a portable remote terminal machine, the time stamp issue server 12 adds time information to the data for a time stamp, and answers the field radio 31 for a round.

[0015]

Time stamp issue request former 21 (requesting agency server) is installed in the round data control pin center,large 20 of a client side. The round field 30 is dotted with the checkpoint and the checkpoint ID sender (short-distance radio equipment) 32 is arranged in each checkpoint, respectively. A round member carries and patrols the field radio 31 which consists of a digital cordless phone (for example, PHS) with a cellular phone with short-distance radio equipment, or short-distance radio equipment etc.

[0016]

Time stamp issue request former 21 of the time stamp issue server 12 of the time stamp processing center 10 and the round data control pin center,large 20 is equipped with the computer apparatus, the communication device, etc. The time stamp issue server 12 and field radio 31 of the time stamp processing center 10 are connected possible [a communication link] through the dial-up line network 41 of the communication link packet network 40, and time stamp issue request former 21 of the round data control pin center,large 20 is connected possible [a communication link] through the Internet 42 of the Internet communication link packet network 40.

[0017]

The short-distance wireless technique which sends the checkpoint ID of a proper from each round checkpoint, respectively is used for the above-mentioned checkpoint ID sender 32, and it has the checkpoint ID which the proper defined, respectively fixed. Furthermore, when

THIS PAGE BLANK (UPTO

raising the unjust prevention function of positional information, it has the function which generates a one-time password. Moreover, the checkpoint ID sender 32 has the function which checks the field radio ID for a round, and the round member ID.

[0018]

The field radio 31 for a round is the cellular phone with which the cellular phone which similarly built in the short-distance wireless sender using a short-distance wireless technique, the digital cordless phone (for example, PHS), or the short-distance wireless sender was attached outside, or a digital cordless phone, in order to communicate with the checkpoint ID sender 32 using a short-distance wireless technique.

[0019]

Drawing 2 is the block diagram of the standard-time time stamp issue server 12 mentioned above, and the time stamp issue server 12 is constituted by CPU12A [which is an operation control section], standard-time synchronous means 12B [which synchronizes with standard time of day], means-of-communications 12C, encryption means 12D, and data input means 12E, information storing section 12F, and ID collating means 12G. CPU12A performs a necessary operation while controlling standard-time synchronous means 12B, means-of-communications 12C, encryption means 12D, and data input means 12E, information storing section 12F, and ID collating means 12G. Standard-time synchronous means 12B accepts the standard time of day from a standard-time dispatch engine, and sets up the time of a criterion. Means-of-communications 12C performs a communication link through the communication link packet network 40 on the radical of control of CPU12A. On the other hand, encryption means 12D calculates a tropism function value, for example, a hash value, based on the command of CPU12A. Data input means 12E inputs various data. Information storing section 12F save the enciphered data, and ID collating means 12G check the effectiveness of License ID.

[0020]

The above-mentioned hash value is a value calculated by the Hash Function which is a tropism function on the other hand, and on the other hand, although it is easy for a tropism function to change and output a certain input, asking from the output of hard flow is a difficult or impossible function. Although a Hash Function is a function which maps a value in a small domain from the big domain in a wide sense, the Hash Function used in a code etc. is a function which has tropism on the other hand and has non-colliding consistency (the probability for a result to become the same that the values which are dimensions differ is low).

[0021]

Drawing 3 is the block diagram of the field radio 31 mentioned above, and the field radio 31 is constituted by external-interface 31A, communications control section 31B, speech processing section 31C, transceiver section 31D, and panel interface 31E, control-section 31F, ROM31G, RAM31H, and clock section 31I. External-interface 31A is transmitted and received between the checkpoint ID senders 32 which are external communication devices. Communications control section 31B controls speech processing section 31C and transceiver section 31D. On the radical of control of communications control section 31B, transceiver section 31D transmits and receives information between means-of-communications 12C of the time stamp issue server 12. Control-section 31F control panel interface 31E, ROM31G, and RAM31H.

[0022]

Drawing 4 is the block diagram of the checkpoint ID sender 32 mentioned above, the checkpoint ID sender 32 has one-time password generation means 32A, application CPU32B, interface function section 32C, ROM32D, and RAM32E, and panel interface 32F and clock section 32G are installed if needed. Application CPU32B controls one-time password generation means 32A, interface function section 32C, ROM32D, RAM32E, and panel interface 32F. One-time password generation means 32A has the function which generates the one-time password for raising the unjust prevention function of positional information. Moreover, the checkpoint ID sender 32 has the function which checks a field radio ID and Round ID.

[0023]

Above-mentioned interface function section 32C transmits and receives information between transceiver section 31D of a field radio 31, and location ID information is stored in ROM32D.

[0024]

the patrol recorder system of drawing 1 -- setting -- a round member -- each checkpoint -- him, such as the field radio ID for a round, and the round member ID, -- confirmed information is transmitted to the checkpoint ID sender 32, and transmission of a checkpoint ID is required of this checkpoint ID sender 32. the checkpoint ID sender 32 -- him, such as the field radio ID for a round, and the round member ID, -- the effectiveness of confirmed information is checked and a checkpoint ID (in one-time password use, this is included) is transmitted to the field radio 31 for a round. If a checkpoint ID is received, the field radio 31 for a round will transmit the transmitting time of day in the clock which a checkpoint ID, and the round member ID and field radio 31 self for a round have in the time stamp issue server 12 which the system which cooperates with an independent organization (certificate authority) or it automatically offers, and will require issue of a time stamp.

[0025]

The time stamp issue server 12 of which the time stamp was required checks a checkpoint ID (in one-time password use, this is included), and effectiveness of positional information, checks the field radio ID for a round, and the effectiveness of the round member ID, and generates a time stamp from the time of day which received the time stamp issue demand, and standard time of day. Moreover, the time stamp issue server 12 is changed into a checkpoint location name or a code from a checkpoint ID, generates the data and the time stamp object which were enciphered with the key for off-line verification, and the online verification key in round data, such as a LOGO of a checkpoint ID, a field radio ID and a time stamp, and an independent organization, and distributes it to time stamp issue request former 21 of the round data control pin center, large 20 through the Internet 42 while it answers the demanded field radio 31 in confirmation-of-receipt information. The time stamp object is stored with the language form (for example, data of an XML format) for describing round data to text format or structured data, is an external request, for example, is offered by XML formal data.

[0026]

Moreover, using two unsymmetrical cryptographic keys of a key which can verify the bona fides of round data on-line, the round data is separately enciphered with encryption or each key to a duplex, and an alteration is prevented. The decode key for off-line verification is a key passed in advance to time stamp issue request former 21, and a cryptographic key verifiable on-line [the other cryptographic key for off-line verification and on-line / other] and a decode key are keys managed in the time stamp processing center 10 which is an independent organization as a private key. Time stamp issue request former 21 posts the data of text format or a structured language format from a time stamp object, and utilizes them as round record while it saves the time stamp object sent from the time stamp

THIS PAGE BLANK (USPTO)

processing center 10.

[0027]

In verification of the bona fides of round data, online verification of data bona fides collates the data which transmitted License ID and the time stamp object to the time stamp issue server 12 of the time stamp processing center 10, decrypted information enciphered with the online cipher key (private key) (private key), and decrypted the data enciphered with the data and the offline cipher key (private key) of text format or a structured language format, and answers a letter in a verification result. Off-line verification of data bona fides decrypts the data enciphered with the offline cipher key (private key) using the decode key for off-line verification currently exhibited by time stamp issue request former 21, and collates with the data of text format or a structured language format.

[0028]

In addition, the encryption information for verification enciphered with the private key for independent organization verification can be decoded with the decode key with which it enciphers by the cryptographic key which an independent organization has, and an independent organization has the text information containing time stamp information, a round location ID code and the field radio ID information for a round, or related information. Moreover, the information enciphered with the private key for off-line verification is the information which can encipher the text information containing time stamp information, a round location ID code and the field radio ID information for a round, or related information by the cryptographic key which an independent organization has, and can be decoded by the predetermined server side.

[0029]

Drawing 5 shows the data configuration of a time stamp object, and a time stamp object is constituted by the A section which consists of the checkpoint location name as time stamp information or codes (positional information, checkpoint ID, etc.), a field radio ID, and the round member ID and an independent organization LOGO, the B section which consist of encryption information for online verification (information which enciphered the A section with the private key for off-line verification), and the C section which consist of information enciphered by the secret cryptographic key for off-line verification. The data of the A section are round data and are a language form for describing to text format or structured data. The data of the B section are a key for certificate authority verification, and consist of a cryptographic key and a decode key, a cryptographic key is a private key (secret key), and a decode key is also a private key (secret). The data of the C section are a key for off-line verification, and consist of a cryptographic key and a decode key, a cryptographic key is a private key (secret), and a decode key is a public key.

[0030]

When verification by time stamp issue request former 21 self is needed on employment and business, the data (C section) which enciphered round data with the key for off-line verification are added to a time stamp object, and the decode key is opened to time stamp issue request former 21. In time stamp issue request former 21, it decrypts using the decode key for off-line verification currently exhibited, and it provides so that it can collate with the data of text format or a structured language format.

[0031]

Drawing 6 shows the patrol recorder structure of a system using the private-telephone circuit by other examples of this invention, and the round data control pin center, large 20 is constituted in the patrol recorder system of drawing 6 by the time stamp issue server 24 which cooperates with the cooperation time server 23 which cooperates with time stamp issue request former 21, and the communication link base station 22 and the time server 11 of the time stamp processing center 10, and the time stamp issue server 12 of the time stamp processing center 10. The cooperation time server 23 receives standard time of day from the time server 11 of the time stamp processing center 10, and supplies the standard time of day to the cooperation time stamp issue server 24. If a checkpoint ID is received, the field radio 31 for a round will transmit automatically the transmitting time of day in the clock which a checkpoint ID, and the round member ID and field radio 31 self have in the cooperation time server 24 through a base station 22, and will require issue of a time stamp.

[0032]

The cooperation time stamp issue server 24 of which the time stamp was required checks effectiveness of a checkpoint ID and positional information, checks a checkpoint ID, a field radio ID, and the effectiveness of the round member ID, and generates a time stamp for the time of day which received the time stamp issue demand from standard time of day.

[0033]

Moreover, the cooperation time stamp issue server 24 is changed into a checkpoint location name or a code from a checkpoint ID, generates the data and the time stamp object which were enciphered with the key for off-line verification, and the key for online verification in round data, such as a LOGO of a checkpoint ID, a field radio ID and a time stamp, and an independent organization, and distributes it 21 times time stamp issue request origin while it answers the demanded field radio 31 for a round in confirmation-of-receipt information. Time stamp issue request former 21 posts the data of text format or a structured language format from a time stamp object, and utilizes them as round record while it saves the time stamp object sent from the cooperation time stamp issue server 24.

[0034]

drawing 7, drawing 8, and drawing 9 are the flow Figs. of an object mold patrol recorder system of operation, and are shown in drawing 7 -- as -- step S1 -- the field radio 31 for a round -- him, such as a field radio ID and the round member ID, -- confirmed information is transmitted to the checkpoint ID sender 32, and a checkpoint ID is required. step S2 -- him, such as a checkpoint ID, a field radio ID, and the round member ID, -- transmitting time of day is transmitted to the time stamp issue server 12 by the clock which confirmed information and self have, and time stamp issue is required. Confirmed information is received from the standard-time time stamp issue server 12 at step S3.

[0035]

it is shown in drawing 8 -- as -- the checkpoint ID sender 32 -- step S4 -- it is -- the checkpoint ID demand from the field radio 31 for a round -- receiving -- him -- the effectiveness of confirmed information is checked, when effective, it progresses to step S5 and a one-time password is generated if needed, after that, it progresses to step S6 and the field radio 31 for a round is answered in a one-time password and a checkpoint ID.

[0036]

the standard-time time stamp issue server 12 is shown in drawing 9 -- as -- step S7 -- the time stamp issue demand from the field radio 31 for a round -- receiving -- him -- the effectiveness of confirmed information is checked. The effectiveness of positional information is checked at step S8, when effective, it progresses to step S9 and the time stamp of the receipt time is generated, and the field radio 31 for a round is answered in confirmation-of-receipt information at step S10. Moreover, it changes into a checkpoint location name or a code

THIS PAGE BLANK (USPTO)

from a checkpoint ID at step S11, round data are enciphered at step S12 with the key for off-line verification, and the key for online verification (the B section of drawing 5, the C section), and a time stamp object is generated at step S13.

[0037]

As shown in drawing 10, time stamp issue request former 21 of the round data control pin center, large 10 posts and records round data from the time stamp object sent from the standard-time time stamp issue server 12 at step S14, and saves a time stamp object at step S15.

[0038]

As drawing 11 is an online verification flow Fig. and shows drawing 12 to drawing 11, time stamp issue request former 21 transmits License ID and a time stamp object to the standard-time time stamp issue server 12 at step S16, requires verification, is step S17 and receives the verification result from the time stamp issue server 12.

[0039]

As shown in drawing 12, to the verification demand of the license ID from time stamp issue request former 21, and a time stamp object, the standard-time time stamp issue server 12 checks the effectiveness of License ID at step S18, and when effective, it decodes the B section of a time stamp object with an online private key at step S19. Decode data and the extraction data (the A section of drawing 5) of a time stamp object are collated at step S20, and a verification result (non-altering judgment) is transmitted to time stamp issue request former 21 at step S21.

[0040]

Drawing 13 is an off-line verification flow Fig., and as shown in drawing 13, time stamp issue request former 21 of the round data control pin center, large 10 decodes the C section of a time stamp object with an off-line public key at step S22, and collates decode data and the extraction data (A section) of a time stamp object at step S23.

[0041]

As mentioned above, he is an independent organization in order to prevent the unauthorized use of a checkpoint ID. (certificate authority) A checkpoint ID is set up and the checkpoint ID is not opened to time stamp issue request former 21. Relating of a checkpoint ID and its installation is the recording method by which round persons, such as record, or manager of the time information of the time stamp which a third person publishes, or round location information cannot intervene, when it is moreover altered, it is offer of the time stamp object an alteration is proved with the trace of an alteration that it is, and it is managing only in an independent organization and it serves as round record in which objectivity has the time information of a time stamp, and record of a round location.

[0042]

Moreover, flexible employment can be performed, when carrying out open employment of the round business only at relating of checkpoint ID and its installation outsourcing-origin in outsourcing etc., or when opening relating of a checkpoint ID and its installation to time stamp issue request former 21.

[0043]

[Effect of the Invention]

As explained above, according to the patrol recorder system in connection with this invention Each round point ID transmitted to the field radio for a round on the occasion of a patrol Since it transmits to the time stamp issue server of an independent organization with the walkie-talkie ID for a round, or its owner ID, and the time stamp object to which time of day was given in the time stamp server is generated and it transmits to a predetermined server Since the right time of day which an independent organization has is directly sent to the server which manages round business while the collection of data currently done by the conventional method and management of a record form become unnecessary, injustice, such as an alteration of the time of day in a round person, can be prevented.

[0044]

Moreover, in the position of managing round business according to this invention, simple round time of day etc. is off-line verifiable if needed, and from the time stamp object sent from the independent organization, since the verification in the independent organization by online is also possible, simplicity and dependability can be reconciled, and the credibility over a user can be raised about round business to coincidence.

[Brief Description of the Drawings]

[Drawing 1] The block diagram showing the outline configuration of the patrol recorder system by the example of this invention.

[Drawing 2] The configuration block Fig. of the standard-time time stamp issue equipment of the patrol recorder system by the example of this invention.

[Drawing 3] The configuration block Fig. of the field radio of the patrol recorder system by the example of this invention.

[Drawing 4] The configuration block Fig. of the checkpoint ID sender of the patrol recorder system by the example of this invention.

[Drawing 5] The explanatory view showing the DS of the time stamp object used in the patrol recorder system by the example of this invention.

[Drawing 6] The block diagram showing the outline configuration of the patrol recorder system by other examples of this invention.

[Drawing 7] The flow Fig. of the field radio used in the patrol recorder system by the example of this invention of operation.

[Drawing 8] The flow Fig. of the checkpoint ID sender in the patrol recorder system by the example of this invention of operation.

[Drawing 9] The flow Fig. of the time stamp issue equipment in the patrol recorder system by the example of this invention of operation.

[Drawing 10] The flow Fig. of the time stamp issue request origin in the patrol recorder system by the example of this invention of operation.

[Drawing 11] The online verification flow Fig. of the time stamp issue equipment in the patrol recorder system by the example of this invention.

[Drawing 12] The online verification flow Fig. of the time stamp issue equipment in the patrol recorder system by the example of this invention.

[Drawing 13] The off-line verification flow Fig. of the time stamp issue request origin in the patrol recorder system by the example of this invention.

[Description of Notations]

10 Time Stamp Processing Center Which is Pin Center, large Side

11 Time Server

12 Time Stamp Issue Server

THIS PAGE BLANK (USPTO)

20 Round Data Control Pin Center,large
21 Time Stump Issue Request Origin
22 Base Station
23 Cooperation Time Server
24-Cooperation Time Stump Issue Server
30 Round Field
31 Field Radio for Round
32-Checkpoint ID Sender
40 Packet Communication Network
41 Dial-up Line Network
42 Internet Line Network

[Translation done.]

THIS PAGE BLANK (USPTO)

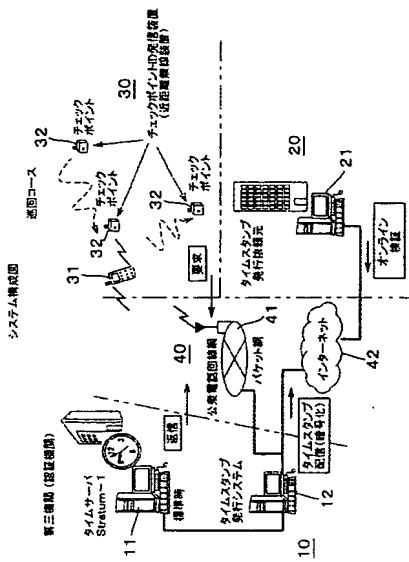
* NOTICES *

JP0 and NCIP1 are not responsible for any damages caused by the use of this translation.

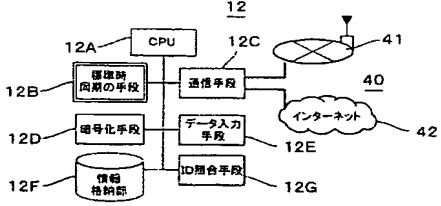
- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

DRAWINGS

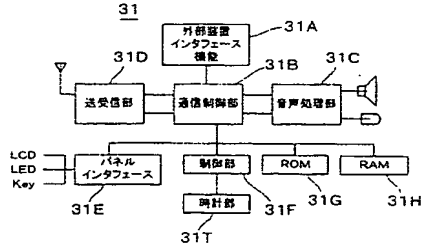
[Drawing 1]



[Drawing 2]

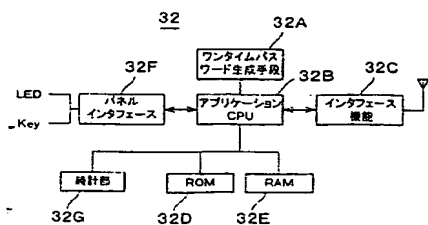


[Drawing 3]

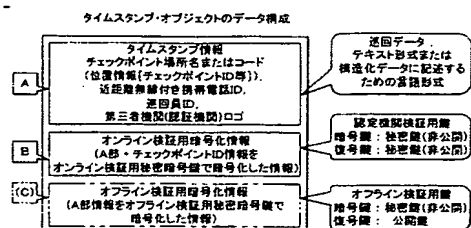


[Drawing 4]

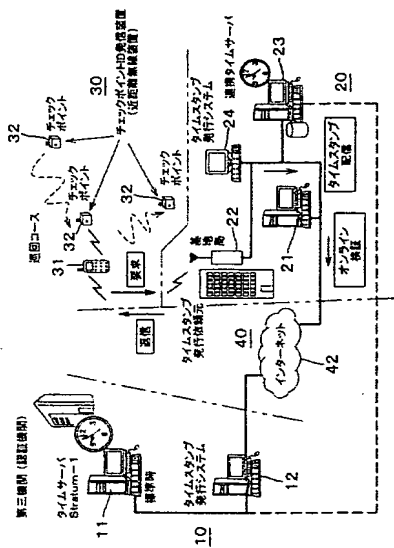
THIS PAGE BLANK (USPTO)



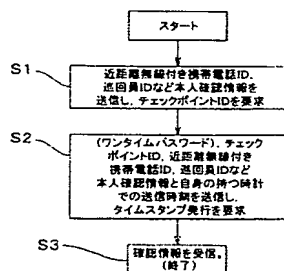
[Drawing 5]



[Drawing 6]

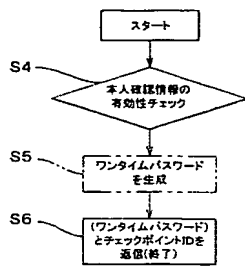


[Drawing 7]

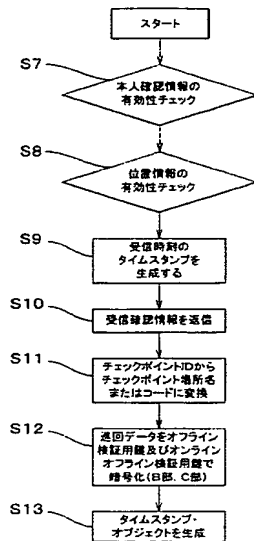


[Drawing 8]

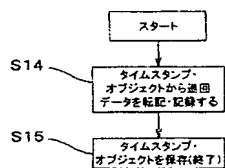
THIS PAGE BLANK (USPTO)



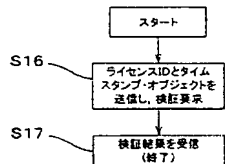
[Drawing 9]



[Drawing 10]

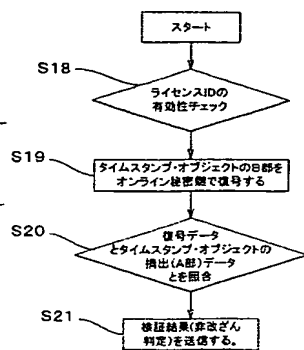


[Drawing 11]

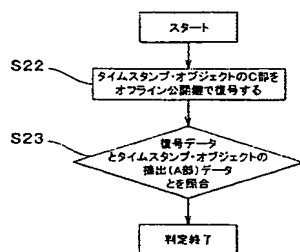


[Drawing 12]

THIS PAGE BLANK (USPTO)



[Drawing 13]



[Translation done.]

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-46305

(P2004-46305A)

(43) 公開日 平成16年2月12日(2004.2.12)

(51) Int. Cl.⁷
G07C 1/20F I
G07C 1/20テーマコード(参考)
3E038

審査請求 未請求 請求項の数 4 O L (全 12 頁)

| | | | |
|-----------|------------------------------|----------|--------------------------------|
| (21) 出願番号 | 特願2002-199415 (P2002-199415) | (71) 出願人 | 000101617 |
| (22) 出願日 | 平成14年7月9日(2002.7.9) | | アマノ株式会社 |
| | | | 神奈川県横浜市港北区大豆戸町275番地 |
| | | (74) 代理人 | 100067714 |
| | | | 弁理士 矢島 正和 |
| | | (72) 発明者 | 横山 純明 |
| | | | 神奈川県横浜市港北区大豆戸町275番地 |
| | | | アマノ株式会社内 |
| | | Fターム(参考) | 3E038 AA01 BA01 BA20 BB05 EA07 |
| | | | GA02 HA05 |

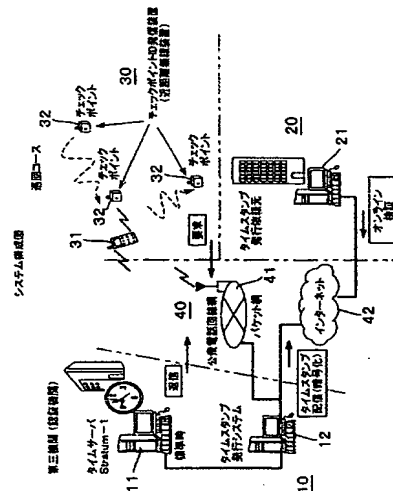
(54) 【発明の名称】 パトロールレコーダシステム

(57) 【要約】

【課題】巡回実施に対する保証を与え、真正性を証明できる簡易にして信頼性の高いパトロールレコーダシステムを提供する。

【解決手段】巡回用携帯無線機31からチェックポイントID発信装置32にチェックポイントIDの送信要求を出し、チェックポイントID発信装置32は、要求者の有効性をチェックし、チェックポイントIDを巡回員に配信する。巡回用携帯無線機31は、タイムスタンプ発行サーバ12にチェックポイントIDと携帯無線機IDを送信しタイムスタンプを要求する。タイムスタンプ発行サーバ12は、要求の有効性をチェックし、標準時刻からタイムスタンプを生成し、それを巡回データ管理センター10のタイムスタンプ発行依頼元21に送信する。タイムスタンプ発行依頼元21は、送られてきたタイムスタンプオブジェクトを保存し、タイムスタンプオブジェクトから巡回データを転記して、巡回記録として活用する。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

タイムスタンプを発行処理するタイムスタンプ処理センターと、タイムスタンプを上記タイムスタンプ処理センターに発行依頼すると共に、巡回員が巡回して得たデータを管理する巡回データ管理センターと、巡回員が巡回すべき巡回領域とからなり、巡回員が携帯用端末機を所持してチェックポイントを巡回し、巡回したチェックポイントの位置情報とその巡回時刻とを記録機へ送信し、記録するように構成したパトロールレコーダシステムであって、

巡回用携帯無線機と、巡回位置に設けられたチェックポイント ID 発信装置と、タイムスタンプ発行サーバとで構成され、

上記巡回用携帯無線機は、無線により上記チェックポイント ID 発信装置に対して ID コードのコールをする ID コール手段と、該 ID コールに呼応してチェックポイント ID 発信装置から発信されるチェックポイント ID コードを受信する ID コード受信手段と、送られて来たチェックポイント ID と巡回用携帯無線機 ID および又は巡回員 ID を上記タイムスタンプ発行サーバに対して無線で送付し、且つ、タイムスタンプをすべき要求をタイムスタンプ発行サーバに対して行うタイムスタンプ発行要求手段とを有し、

上記チェックポイント ID 発信装置は、巡回位置を示す ID コード記憶手段と、上記巡回用携帯無線機からの ID コールに応答して ID を発信する巡回位置 ID 発信手段とを有し、

上記タイムスタンプ発行サーバは、標準時刻を刻む時計手段と、巡回用携帯無線機から送られてきた上記 ID コードに対してその時刻を付加し、且つ、暗号化されたタイムスタンプオブジェクトを生成して所定のサーバに送信するタイムスタンプオブジェクト発行手段とを有する、

ことを特徴とするパトロールレコーダシステム。

【請求項 2】

タイムスタンプオブジェクトの構成が、タイムスタンプ情報および巡回位置 ID および巡回用携帯無線機 ID および又は巡回員 ID 或は関連情報を含むテキスト情報と、上記テキスト情報を第三者機関検証用秘密鍵で暗号化されたオンライン検証用暗号化情報と、上記テキスト情報をオフライン検証用秘密鍵で暗号化された情報とで構成されていることを特徴とする請求項 1 に記載のパトロールレコーダシステム。

【請求項 3】

上記タイムスタンプ処理センターは、標準時刻を供給するタイムサーバと、該タイムサーバが供給する時刻を基にタイムスタンプを発行処理するタイムスタンプ発行サーバからなり、上記巡回データ管理センターは、上記タイムスタンプ処理センターのタイムスタンプ発行サーバにタイムスタンプを依頼するタイムスタンプ発行依頼元からなることを特徴とする請求項 1 又は 2 に記載のパトロールレコーダシステム。

【請求項 4】

上記巡回データ管理センターは、さらに、上記タイムスタンプ処理センターのタイムサーバに連携する連携タイムサーバと、上記タイムスタンプ発行サーバと連携する連携タイムスタンプ発行サーバからなり、上記巡回用携帯無線機は、無線により上記チェックポイント ID 発信装置に対して ID コードのコールをする ID コール手段と、該 ID コールに呼応してチェックポイント ID 発信装置から発信されるチェックポイント ID コードを受信する ID コード受信手段と、送られてきたチェックポイント ID と巡回用携帯無線機 ID および又は巡回員 ID を上記タイムスタンプ処理センターのタイムスタンプ発行サーバと連携するタイムスタンプ発行サーバに対して無線で送付し、且つ、タイムスタンプをすべき要求を行うタイムスタンプ発行要求手段とを有することを特徴とする請求項 1、2 又は 3 に記載のパトロールレコーダシステム。

【発明の詳細な説明】**【0001】****【発明の属する技術分野】**

10

20

30

40

50

本発明は、工場とか倉庫あるいはビル、学校といった各種施設の防犯警備パトロール等に用いられ、各巡回箇所における時刻を記録し、又、その証明を可能にするパトロールレコーダシステムに関するものである。

【0002】

【従来の技術】

従来のパトロールレコーダシステムとして、本出願人によって提案された特開昭61-82288号公報に見られる「巡回記録装置」がある。この装置は、携帯式のパトロールレコーダシステムであって、巡回中に巡回場所に設置されたコード器からポジションコードが付されると共に、巡回時刻をレコーダ内に記録し、セントラルユニットにおいて上記パトロールレコーダシステムに記録巡回箇所のコードと巡回時刻データを収集する構成と成

10

【0003】

また、特開平9-305813号公報に記載の「建物運営管理装置」も存在する。この装置は、保守員が所持する携帯機の位置の変化を示す位置変化情報を送信する構内交換器機と、この構内交換機と電話回線により接続された管理装置とが設置された装置において、上記管理装置に上記位置変化情報を受信して上記保守員の巡回時間を算出する巡回時間算出手段を備えたものであって、携帯機から位置情報を検知し、巡回場所と巡回時間を収集するシステムである。

【0004】

【発明が解決しようとする課題】

上記従来のシステムでは、時刻の正確性、悪意に基づく時刻の改ざんに対しては何ら信頼性がおけないものであり、巡回実施に対する保証を与えることができない問題がある。即ち、タイムスタンプの記録は、パトロールレコーダ装置の内蔵する時計、あるいはGPS時計、電波時計で同期させた時刻であっても、それに同期していたことを証明するものではなく、第三者が認めるものではなかった。

20

また、警備などを請け負った企業・団体が本当に巡回したことを証明するにあたり、請け負った企業・団体が管理する時刻や第三者機関（認証機関）の発行したタイムスタンプであっても、テキストデータでは改ざんできる可能性があるため、真正性を証明できるものではなかった。更に、その他の巡回データも同様に改ざんできる可能性があり、真正性を証明できるものではなかった。

30

【0005】

更に、携帯電話またはデジタルコードレスホンを使い、GPSで場所情報を付加して、タイムスタンプを第三者機関に要求する方式も考えられるが、GPSによる場所情報は公開情報であるため、場所のなりすまし（改ざん）が可能であり、真正性を証明できるものではない。

また携帯電話またはデジタルコードレスホンを使い、GPSで第三者機関がその場所を捕捉する方式もあるが、GPSによる場所捕捉は、地下街、ビル内など捕捉できない環境も多く、位置を特定するには、位置を捕捉する代替システムが必要になるなどの問題がある。

【0006】

本発明は、上述の問題点を鑑みてなされたもので、その目的は、巡回実施に対する保証を与え、真正性を証明できるように工夫した簡易にして信頼性の高いパトロールレコーダシステムを提供することである。

40

【0007】

【課題を解決するための手段】

上記目的を達成するために、本発明のパトロールレコーダシステムは、前記請求項1に記載の如く、タイムスタンプを発行処理するタイムスタンプ処理センターと、タイムスタンプを上記タイムスタンプ処理センターに発行依頼すると共に、巡回員が巡回して得たデータを管理する巡回データ管理センターと、巡回員が巡回すべき巡回領域とからなり、巡回員が携帯用端末機を所持してチェックポイントを巡回し、巡回したチェックポイントの位

50

置情報とその巡回時刻とを記録機へ送信し、記録するように構成したパトロールレコーダシステムであって、巡回用携帯無線機と、巡回位置に設けられたチェックポイントID発信装置と、タイムスタンプ発行サーバとで構成され、上記巡回用携帯無線機は、無線により上記チェックポイントID発信装置に対してIDコードのコールをするIDコール手段と、該IDコールに呼応してチェックポイントID発信装置から発信されるチェックポイントIDコードを受信するIDコード受信手段と、送られて来たチェックポイントIDと巡回用携帯無線機IDおよび又は巡回員IDを上記タイムスタンプ発行サーバに対して無線で送付し、且つ、タイムスタンプをすべき要求をタイムスタンプ発行サーバに対して行うタイムスタンプ発行要求手段とを有し、上記チェックポイントID発信装置は、巡回位置を示すIDコード記憶手段と、上記巡回用携帯無線機からのIDコールに応答してIDを発信する巡回位置ID発信手段とを有し、上記タイムスタンプ発行サーバは、標準時刻を刻む時計手段と、巡回用携帯無線機から送られてきた上記IDコードに対してその時刻を付加し、且つ、暗号化されたタイムスタンプオブジェクトを生成して所定のサーバに送信するタイムスタンプオブジェクト発行手段とを有することを特徴とする。

【0008】

また、本発明のパトロールレコーダシステムは、前記請求項2に記載の如く、タイムスタンプオブジェクトの構成が、タイムスタンプ情報および巡回位置IDおよび巡回用携帯無線機IDおよび又は巡回員ID或は関連情報を含むテキスト情報と、上記テキスト情報を第三者機関検証用秘密鍵で暗号化されたオンライン検証用暗号化情報と、上記テキスト情報をオフライン検証用秘密鍵で暗号化された情報とで構成されていることを特徴とする。

【0009】

さらに、本発明のパトロールレコーダシステムは、前記請求項3に記載の如く、上記タイムスタンプ処理センターは、標準時刻を供給するタイムサーバと、該タイムサーバが供給する時刻を基にタイムスタンプを発行処理するタイムスタンプ発行サーバからなり、上記巡回データ管理センターは、上記タイムスタンプ処理センターのタイムスタンプ発行サーバにタイムスタンプを依頼するタイムスタンプ発行依頼元からなることを特徴とする。

【0010】

さらに、本発明のパトロールレコーダシステムは、前記請求項4に記載の如く、上記巡回データ管理センターは、さらに、上記タイムスタンプ処理センターのタイムサーバに連携する連携タイムサーバと、上記タイムスタンプ発行サーバと連携する連携タイムスタンプ発行サーバからなり、上記巡回用携帯無線機は、無線により上記チェックポイントID発信装置に対してIDコードのコールをするIDコール手段と、該IDコールに呼応してチェックポイントID発信装置から発信されるチェックポイントIDコードを受信するIDコード受信手段と、送られてきたチェックポイントIDと巡回用携帯無線機IDおよび又は巡回員IDを上記タイムスタンプ処理センターのタイムスタンプ発行サーバと連携するタイムスタンプ発行サーバに対して無線で送付し、且つ、タイムスタンプをすべき要求を行うタイムスタンプ発行要求手段とを有することを特徴とする。

【0011】

上記の各手段から成る本発明によれば、各巡回チェックポイントに、夫々、固有のチェックポイントID（位置情報）を発信する近距離無線技術を使ったチェックポイントID発信装置を設置し、また巡回員が近距離無線付き携帯電話または近距離発信装置付きデジタルコードレスホン等の携帯無線機を持って巡回する。巡回員がチェックポイントで携帯無線機からチェックポイントID発信装置にチェックポイントID（位置情報）の送信要求を出し、チェックポイントID発信装置は、要求者の有効性をチェックし、有効である場合にチェックポイントIDを巡回員に配信する。

【0012】

次に携帯無線機は、チェックポイントIDを受信すると、自動的にタイムスタンプ発行サーバにチェックポイントIDと携帯無線機IDおよび又は巡回員IDを送信し、タイムスタンプ発行システムにタイムスタンプを要求する。タイムスタンプを要求されたタイムスタンプ発行サーバは、要求の有効性をチェックし、有効である場合に受信確認情報を返信

するとともに、標準時刻からタイムスタンプを生成し、それを巡回データ管理センターのタイムスタンプ発行依頼元へ送信する。タイムスタンプ発行依頼元は、送られてきたタイムスタンプ（オブジェクト）を保存し、タイムスタンプオブジェクトから巡回データを転記して、巡回記録として活用する。

【0013】

また、巡回データの真正性の検証にあたって、タイムスタンプオブジェクトを第三者機関（認証機関）であるタイムスタンプ処理センターに通信で送信し、検証用に暗号化された情報を復号化（秘密鍵）、照合・検証し、オンラインで検証結果を返信する。また、タイムスタンプ発行依頼元自身による検証が運用および業務上必要となる場合は、タイムスタンプオブジェクトに巡回データをオフライン検証用鍵で暗号化した情報を付加することにより、タイムスタンプ発行依頼元で、公開されているオフライン検証用復号鍵を使って照合、検証することを可能にする。

【0014】

【発明の実施の形態】

以下に、本発明の実施例によるパトロールレコーダシステムについて、図面を参照しながら説明する。図1は本発明の実施例によるパトロールレコーダシステムの概略構成を示し、図中、10は外部機関としてのタイムスタンプ処理センター、20はクライアント側の巡回データ管理センター、30は巡回員が各チェックポイントを巡回する巡回領域である。タイムスタンプ処理センター10は、世界時に同期しているタイムサーバ11及びタイムスタンプ発行サーバ12から成り、タイムスタンプを検証する。センター側のタイムサーバ11は、協定世界時に同期しており、タイムスタンプ発行サーバ12に対して時刻の配信を行う。タイムスタンプ発行サーバ12は、携帯用端末機である巡回用携帯無線機31から要求されたタイムスタンプ発行要求に対し、タイムスタンプ対象データに時刻情報を付加して、巡回用携帯無線機31に返信する。

【0015】

クライアント側の巡回データ管理センター20には、タイムスタンプ発行依頼元21（依頼元サーバ）が設置されている。巡回領域30にはチェックポイントが点在しており、各チェックポイントには、それぞれチェックポイントID発信装置（近距離無線装置）32が配設されている。巡回員は、近距離無線装置付き携帯電話または近距離無線装置付きデジタルコードレスホン（例えばPHS）等からなる携帯無線機31を携帯して巡回する。

【0016】

タイムスタンプ処理センター10のタイムスタンプ発行サーバ12、及び、巡回データ管理センター20のタイムスタンプ発行依頼元21は、コンピュータ装置や通信装置等を備えている。タイムスタンプ処理センター10のタイムスタンプ発行サーバ12と携帯無線機31とは、通信パケット網40の公衆電話回線網41を通して通信可能に接続されており、巡回データ管理センター20のタイムスタンプ発行依頼元21は、インターネット通信パケット網40のインターネット42を介して通信可能に接続されている。

【0017】

上記のチェックポイントID発信装置32は、各巡回チェックポイントからそれぞれ固有のチェックポイントIDを発信する近距離無線技術を使ったものであり、それぞれ定められた固有の固定したチェックポイントIDを有している。更に、位置情報の不正防止機能を高める場合は、ワンタイムパスワードを生成する機能を有する。また、チェックポイントID発信装置32は巡回用携帯無線機IDと巡回員IDをチェックする機能を有する。

【0018】

巡回用携帯無線機31は、近距離無線技術を使ったチェックポイントID発信装置32と交信するために、同じく近距離無線技術を使った近距離無線発信装置を内蔵した携帯電話またはデジタルコードレスホン（例えば、PHS）、又は近距離無線発信装置が外部に取付けられた携帯電話またはデジタルコードレスホンである。

【0019】

図2は前述した標準時タイムスタンプ発行サーバ12のブロック図であって、タイムスタ

ンプ発行サーバ12は、演算制御部であるCPU12A、標準時刻に同期する標準時同期手段12B、通信手段12C、暗号化手段12D、データ入力手段12E、情報格納部12F、及びID照合手段12Gによって構成されている。CPU12Aは、標準時同期手段12B、通信手段12C、暗号化手段12D、データ入力手段12E、情報格納部12FおよびID照合手段12Gを制御するとともに、所要の演算を行う。標準時同期手段12Bは標準時発信機関からの標準時刻を受け入れ、標準時を設定する。通信手段12Cは、CPU12Aの制御の基に通信パケット網40を介して通信を実行する。暗号化手段12DはCPU12Aの指令に基づいて一方向性関数値例えばハッシュ値を演算する。データ入力手段12Eは各種データを入力する。情報格納部12Fは暗号化されたデータを保存し、ID照合手段12GはライセンスIDの有効性をチェックする。

10

【0020】

上記のハッシュ値は、一方向性関数であるハッシュ関数によって演算された値であって、一方向性関数は、ある入力を変換し出力するのは簡単であるが逆方向の出力から求めることが困難もしくは不可能な関数である。ハッシュ関数は、広義には大きな定義域から小さな定義域に値を写像する関数であるが、暗号などで利用されるハッシュ関数は、一方向性を持ち、非衝突一致性が有る（元の値が異なるのに結果が同一になる確率が低い）関数である。

【0021】

図3は前述した携帯無線機31のブロック図であって、携帯無線機31は、外部インターフェース31A、通信制御部31B、音声処理部31C、送受信部31D、パネルインターフェース31E、制御部31F、ROM31G、RAM31Hおよび時計部31Tによって構成されている。外部インターフェース31Aは外部の通信装置であるチェックポイントID発信装置32との間で送受信する。通信制御部31Bは音声処理部31Cと送受信部31Dを制御する。送受信部31Dは通信制御部31Bの制御の基に、タイムスタンプ発行サーバ12の通信手段12Cとの間で情報の送受信を行う。制御部31Fは、パネルインターフェース31EとROM31GおよびRAM31Hを制御する。

20

【0022】

図4は前述したチェックポイントID発信装置32のブロック図であって、チェックポイントID発信装置32は、ワнтаイムパスワード生成手段32A、アプリケーションCPU32B、インターフェース機能部32C、ROM32DおよびRAM32Eを有し、必要に応じてパネルインターフェース32Fと時計部32Gが設置される。アプリケーションCPU32Bは、ワнтаイムパスワード生成手段32A、インターフェース機能部32C、ROM32D、RAM32E、およびパネルインターフェース32Fを制御する。ワнтаイムパスワード生成手段32Aは、位置情報の不正防止機能を高めるためのワнтаイムパスワードを生成する機能を有する。また、チェックポイントID発信装置32は、携帯無線機IDと巡回IDをチェックする機能を有する。

30

【0023】

上記のインターフェース機能部32Cは、携帯無線機31の送受信部31Dとの間で情報の送受信を行い、ROM32Dには位置ID情報が格納されている。

【0024】

図1のパトロールレコーダシステムにおいて、巡回員が各チェックポイントで巡回用携帯無線機IDおよび巡回員IDなどの本人確認情報を、チェックポイントID発信装置32に送信し、該チェックポイントID発信装置32にチェックポイントIDの送信を要求する。チェックポイントID発信装置32は、巡回用携帯無線機IDおよび巡回員IDなどの本人確認情報の有効性をチェックし、巡回用携帯無線機31にチェックポイントID（ワнтаイムパスワード使用の場合これを含む）を送信する。巡回用携帯無線機31は、チェックポイントIDを受信すると、自動的に第三者機関（認証機関）またはそれと連携するシステムが提供するタイムスタンプ発行サーバ12に、チェックポイントID、巡回員ID、巡回用携帯無線機31自身の持つ時計での送信時刻を送信し、タイムスタンプの発行を要求する。

40

50

【0025】

タイムスタンプを要求されたタイムスタンプ発行サーバ12は、チェックポイントID（ワンタイムパスワード使用の場合これを含む）と、位置情報の有効性のチェックを行い、巡回用携帯無線機ID、巡回員IDの有効性をチェックし、タイムスタンプ発行要求を受信した時刻と、標準時刻からタイムスタンプを生成する。また、タイムスタンプ発行サーバ12は、要求してきた携帯無線機31に受信確認情報を返信するとともに、チェックポイントIDからチェックポイント場所名またはコードに変換し、チェックポイントID、携帯無線機IDおよびタイムスタンプ、第三者機関のロゴなどの巡回データをオフライン検証用鍵およびオンライン検証鍵で暗号化されたデータとタイムスタンプオブジェクトを生成し、それを巡回データ管理センター20のタイムスタンプ発行依頼元21に、インターネット42を通して配信する。タイムスタンプオブジェクトは、巡回データをテキスト形式または構造化データに記述するための言語形式（例えば、XML形式のデータ）で格納しており、外部要求で、例えばXML形式データで提供する。

10

【0026】

また、巡回データの真正性をオンラインで検証できる鍵の二つの非対称暗号鍵を使って、その巡回データを二重に暗号化、あるいは個々の鍵で別々に暗号化して改ざんを防止する。オフライン検証用の復号鍵は事前にタイムスタンプ発行依頼元21に渡しておく鍵で、その他のオフライン検証用暗号鍵およびオンラインで検証できる暗号鍵、復号鍵は秘密鍵として第三者機関であるタイムスタンプ処理センター10で管理する鍵である。タイムスタンプ発行依頼元21は、タイムスタンプ処理センター10から送られてきたタイムスタンプオブジェクトを保存するとともに、タイムスタンプオブジェクトからテキスト形式または構造化言語形式のデータを転記して、巡回記録として活用する。

20

【0027】

巡回データの真正性の検証にあたって、データ真正性のオンライン検証は、ライセンスIDとタイムスタンプオブジェクトを、タイムスタンプ処理センター10のタイムスタンプ発行サーバ12に送信し、オンライン暗号鍵（秘密鍵）で暗号化された情報を復号化（秘密鍵）し、テキスト形式または構造化言語形式のデータおよびオフライン暗号鍵（秘密鍵）で暗号化されたデータを復号化したデータとを照合し、検証結果を返信する。データ真正性のオフライン検証は、タイムスタンプ発行依頼元21で公開されているオフライン検証用の復号鍵を使ってオフライン暗号鍵（秘密鍵）で暗号化されたデータを復号化し、テキスト形式または構造化言語形式のデータと照合する。

30

【0028】

尚、第三者機関検証用秘密鍵で暗号化された検証用暗号化情報は、タイムスタンプ情報および巡回位置IDコードおよび巡回用携帯無線機ID情報または関連情報を含むテキスト情報を、第三者機関が有する暗号鍵で暗号化し、且つ、第三者機関が有する復号鍵で復号が可能である。また、オフライン検証用秘密鍵で暗号化された情報は、タイムスタンプ情報および巡回位置IDコードおよび巡回用携帯無線機ID情報または関連情報を含むテキスト情報を、第三者機関が有する暗号鍵で暗号化し、且つ、所定サーバ側で復号可能な情報である。

【0029】

図5は、タイムスタンプオブジェクトのデータ構成を示すもので、タイムスタンプオブジェクトは、タイムスタンプ情報としてのチェックポイント場所名またはコード（位置情報、チェックポイントID等）、携帯無線機ID、巡回員ID、第三者機関ロゴからなるA部と、オンライン検証用暗号化情報（A部をオフライン検証用秘密鍵で暗号化した情報）からなるB部、およびオフライン検証用秘密暗号鍵で暗号化した情報からなるC部によって構成されている。A部のデータは巡回データであり、テキスト形式または構造化データに記述するための言語形式である。B部のデータは認証機関検証用鍵であり、暗号鍵と復号鍵からなり、暗号鍵は秘密鍵（非公開鍵）であり、復号鍵も秘密鍵（非公開）である。C部のデータはオフライン検証用鍵であり、暗号鍵と復号鍵からなり、暗号鍵は秘密鍵（非公開）であり、復号鍵は公開鍵である。

40

50

【0030】

タイムスタンプ発行依頼元21自身による検証が運用、業務上必要となる場合は、タイムスタンプオブジェクトに巡回データをオフライン検証用鍵で暗号化したデータ(C部)を付加し、その復号鍵をタイムスタンプ発行依頼元21に公開する。タイムスタンプ発行依頼元21では、公開されているオフライン検証用復号鍵を使って復号化し、テキスト形式または構造化言語形式のデータと照合できるように提供する。

【0031】

図6は、本発明の他の実施例による構内電話回線を用いたパトロールレコーダシステムの構成を示し、図6のパトロールレコーダシステムにおいて、巡回データ管理センター20は、タイムスタンプ発行依頼元21と、通信基地局22とタイムスタンプ処理センター10のタイムサーバ11と連携する連携タイムサーバ23、および、タイムスタンプ処理センター10のタイムスタンプ発行サーバ12と連携するタイムスタンプ発行サーバ24によって構成される。連携タイムサーバ23は、タイムスタンプ処理センター10のタイムサーバ11から標準時刻を受け、その標準時刻を連携タイムスタンプ発行サーバ24に供給する。巡回用携帯無線機31は、チェックポイントIDを受信すると、基地局22を介して連携タイムサーバ24に、チェックポイントID、巡回員ID、携帯無線機31自身の持つ時計での送信時刻を自動的に送信し、タイムスタンプの発行を要求する。

【0032】

タイムスタンプを要求された連携タイムスタンプ発行サーバ24は、チェックポイントID、位置情報の有効性のチェックを行い、チェックポイントID、携帯無線機ID、巡回員IDの有効性をチェックし、タイムスタンプ発行要求を受信した時刻を標準時刻からタイムスタンプを生成する。

【0033】

また、連携タイムスタンプ発行サーバ24は、要求してきた巡回用携帯無線機31に受信確認情報を返信すると共に、チェックポイントIDからチェックポイント場所名またはコードに変換し、チェックポイントID、携帯無線機IDおよびタイムスタンプ、第三者機関のロゴなどの巡回データをオフライン検証用鍵およびオンライン検証用鍵で暗号化されたデータとタイムスタンプオブジェクトを生成し、それをタイムスタンプ発行依頼元21配信する。タイムスタンプ発行依頼元21は、連携タイムスタンプ発行サーバ24から送られてきたタイムスタンプオブジェクトを保存すると共に、タイムスタンプオブジェクトからテキスト形式または構造化言語形式のデータを転記して、巡回記録として活用する。

【0034】

図7、図8および図9は、オブジェクト型パトロールレコーダシステムの動作フロー図であって、図7に示すようにステップS1で巡回用携帯無線機31は携帯無線機ID、巡回員IDなどの本人確認情報をチェックポイントID発信装置32に送信し、チェックポイントIDを要求する。ステップS2で、チェックポイントID、携帯無線機ID、巡回員IDなどの本人確認情報と自身の持つ時計で送信時刻をタイムスタンプ発行サーバ12に送信し、タイムスタンプ発行を要求する。ステップS3で標準時タイムスタンプ発行サーバ12から確認情報を受信する。

【0035】

図8に示すように、チェックポイントID発信装置32は、ステップS4で、巡回用携帯無線機31からのチェックポイントID要求に対して、本人確認情報の有効性をチェックし、有効な場合にステップS5に進んで必要に応じてワンタイムパスワードを生成し、その後、ステップS6に進んでワンタイムパスワードとチェックポイントIDを巡回用携帯無線機31に返信する。

【0036】

標準時タイムスタンプ発行サーバ12は、図9に示すように、ステップS7で巡回用携帯無線機31からのタイムスタンプ発行要求に対して、本人確認情報の有効性をチェックする。ステップS8で位置情報の有効性をチェックし、有効な場合にステップS9に進み受信時刻のタイムスタンプを生成し、ステップS10で受信確認情報を巡回用携帯無線機3

1に返信する。また、ステップS 1 1でチェックポイントIDからチェックポイント場所名またはコードに変換し、ステップS 1 2で巡回データをオフライン検証用鍵およびオンライン検証用鍵で暗号化（図5のB部、C部）し、ステップS 1 3でタイムスタンプオブジェクトを生成する。

【0037】

図10に示すように、巡回データ管理センター10のタイムスタンプ発行依頼元21は、ステップS 1 4で標準時タイムスタンプ発行サーバ12から送られてきたタイムスタンプオブジェクトから巡回データを転記・記録し、ステップS 1 5でタイムスタンプオブジェクトを保存する。

【0038】

図11は図12はオンライン検証フロー図であって、図11に示すように、タイムスタンプ発行依頼元21は、ステップS 1 6でライセンスIDとタイムスタンプオブジェクトを標準時タイムスタンプ発行サーバ12に送信して検証を要求し、ステップS 1 7で、タイムスタンプ発行サーバ12からの検証結果を受信する。

【0039】

図12に示すように、標準時タイムスタンプ発行サーバ12はタイムスタンプ発行依頼元21からのライセンスIDとタイムスタンプオブジェクトの検証要求に対して、ステップS 1 8でライセンスIDの有効性をチェックし、有効な場合にステップS 1 9でタイムスタンプオブジェクトのB部をオンライン秘密鍵で復号する。ステップS 2 0で復号データとタイムスタンプオブジェクトの抽出データ（図5のA部）とを照合し、ステップS 2 1で、検証結果（非改ざん判定）をタイムスタンプ発行依頼元21に送信する。

【0040】

図13はオフライン検証フロー図であって、図13に示すように、巡回データ管理センター10のタイムスタンプ発行依頼元21は、ステップS 2 2でタイムスタンプオブジェクトのC部をオフライン公開鍵で復号し、ステップS 2 3で復号データとタイムスタンプオブジェクトの抽出データ（A部）とを照合する。

【0041】

以上のように、チェックポイントIDの不正使用を防ぐために、第三者機関（認証機関）でチェックポイントIDを設定し、そのチェックポイントIDは、タイムスタンプ発行依頼元21に公開しない。チェックポイントIDとその設置場所の関係付けは、第三者機関のみで管理することで、第三者が発行するタイムスタンプの時刻情報や巡回場所情報の記録など巡回者や管理者が介在できない記録方式で、しかも改ざんすると改ざんの痕跡で改ざんが判明するタイムスタンプオブジェクトの提供で、タイムスタンプの時刻情報や巡回場所の記録が客観性のある巡回記録となる。

【0042】

また、巡回業務を業務委託などの場合は、チェックポイントIDとその設置場所の関係付けを業務委託元にだけ公開運用する場合や、チェックポイントIDとその設置場所の関係付けをタイムスタンプ発行依頼元21に公開する場合など、柔軟な運用ができる。

【0043】

【発明の効果】

以上に説明したように、本発明にかかわるパトロールレコーダシステムによれば、パトロールに際して巡回用携帯無線機に送信される各巡回ポイントIDを、巡回用無線機ID又はその所有者IDと共に第三者機関のタイムスタンプ発行サーバに送信し、タイムスタンプサーバにて時刻が付与されたタイムスタンプオブジェクトを生成して所定のサーバに送信するので、従来の方式で行われていたデータの収集作業や、記録用紙の管理とかが不要になると共に、第三者機関の有する正しい時刻が巡回業務を管理するサーバに直接送られてくるから、巡回者における時刻の改ざん等の不正を防止できる。

【0044】

また、本発明によれば巡回業務を管理する立場においては、第三者機関から送られたタイムスタンプオブジェクトから、必要に応じてオフラインにて簡易的な巡回時刻等の検証を

10

20

30

40

50

行い、又、オンラインによる第三者機関における検証も可能であるから、簡易性と信頼性とを両立させることができ、同時に巡回業務に関して客先に対する信用度を向上させることができる。

【図面の簡単な説明】

【図 1】本発明の実施例によるパトロールレコーダシステムの概略構成を示すブロック図。

【図 2】本発明の実施例によるパトロールレコーダシステムの標準時タイムスタンプ発行装置の構成ブロック図。

【図 3】本発明の実施例によるパトロールレコーダシステムの携帯無線機の構成ブロック図。

10

【図 4】本発明の実施例によるパトロールレコーダシステムのチェックポイント ID 発信装置の構成ブロック図。

【図 5】本発明の実施例によるパトロールレコーダシステムにおいて用いるタイムスタンプオブジェクトのデータ構造を示す説明図。

【図 6】本発明の他の実施例によるパトロールレコーダシステムの概略構成を示すブロック図。

【図 7】本発明の実施例によるパトロールレコーダシステムにおいて用いる携帯無線機の動作フロー図。

【図 8】本発明の実施例によるパトロールレコーダシステムにおけるチェックポイント ID 発信装置の動作フロー図。

20

【図 9】本発明の実施例によるパトロールレコーダシステムにおけるタイムスタンプ発行装置の動作フロー図。

【図 10】本発明の実施例によるパトロールレコーダシステムにおけるタイムスタンプ発行依頼元の動作フロー図。

【図 11】本発明の実施例によるパトロールレコーダシステムにおけるタイムスタンプ発行装置のオンライン検証フロー図。

【図 12】本発明の実施例によるパトロールレコーダシステムにおけるタイムスタンプ発行装置のオンライン検証フロー図。

【図 13】本発明の実施例によるパトロールレコーダシステムにおけるタイムスタンプ発行依頼元のオフライン検証フロー図。

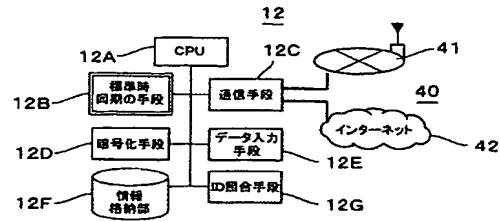
30

【符号の説明】

| | |
|-----|-----------------------|
| 1 0 | センター側であるタイムスタンプ処理センター |
| 1 1 | タイムサーバ |
| 1 2 | タイムスタンプ発行サーバ |
| 2 0 | 巡回データ管理センター |
| 2 1 | タイムスタンプ発行依頼元 |
| 2 2 | 基地局 |
| 2 3 | 連携タイムサーバ |
| 2 4 | 連携タイムスタンプ発行サーバ |
| 3 0 | 巡回領域 |
| 3 1 | 巡回用携帯無線機 |
| 3 2 | チェックポイント ID 発信装置 |
| 4 0 | パケット通信網 |
| 4 1 | 公衆電話回線網 |
| 4 2 | インターネット回線網 |

40

【図 2】



31

31A 外部装置
インタフェース
機能

31D 受信部

31B 通信制御部

31C 音声処理部

31E パネル
インタフェース

31F 制御部

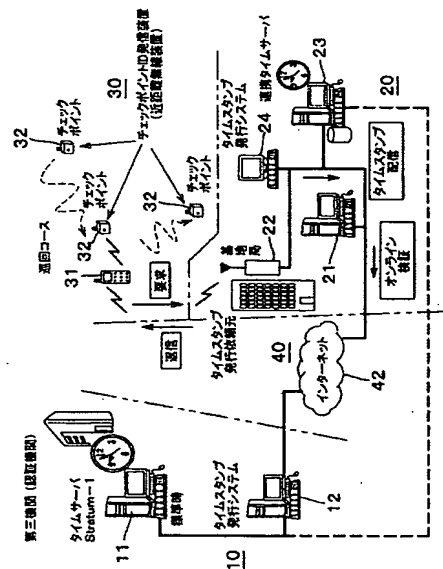
31G ROM

31H RAM

31T 表示部

LCD
LED
Key

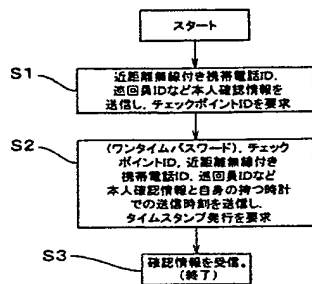
【図 6】



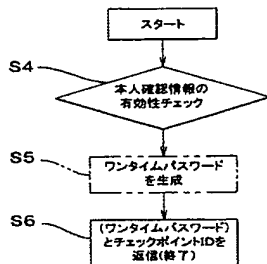
タイムスタンプ・オブジェクトのデータ構成

| | | |
|------------|--|---|
| (A) | <p style="text-align: center;">タイムスタンプ情報</p> <p>チェックポイント場所名またはコード (位置情報(チェックポイントID等))、 近距離検索用IDを携帯電話ID、 巡回員ID、 第三者機関(都道府機関)ロゴ</p> | <p>巡回データ: テキスト形式または 構造化データに記述する ための書式形式</p> |
| (B) | <p style="text-align: center;">オンライン検証用暗号化情報 (A部・チェックポイントID情報も オンライン検証用秘密暗号化ID暗号化した情報)</p> | <p>認定機関発行用 暗号鍵: 秘密鍵(非公認) 復号鍵: 秘密鍵(非公認)</p> |
| (C) | <p style="text-align: center;">オフライン検証用暗号化情報 (A部情報もオフライン検証用秘密暗号鍵で 暗号化した情報)</p> | <p>オフライン検証用 暗号鍵: 秘密鍵(非公認) 復号鍵: 秘密鍵</p> |

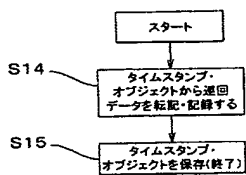
【図 7】



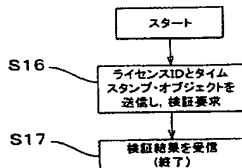
【図 8】



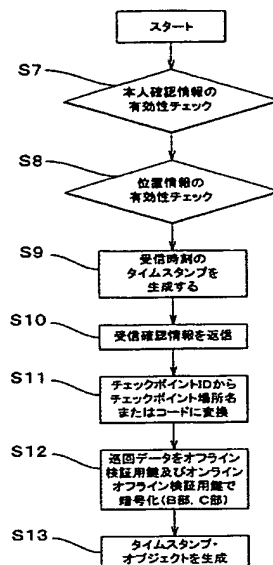
【図 10】



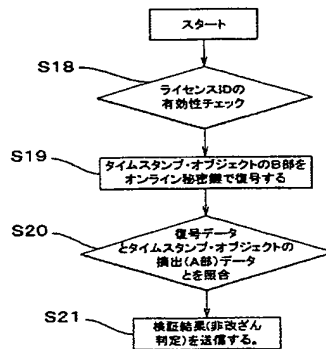
【図 11】



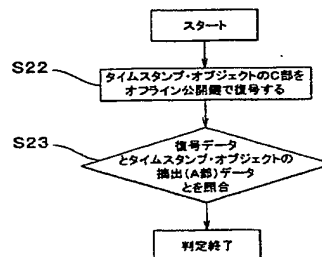
【図 9】



【図 12】



【図 13】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record.**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)